COUNCIL POLICY

ICT SECURITY POLICY

GLENORCHY CITY COUNCIL

PURPOSE

The purpose of this policy is to establish and maintain a consistent and responsive framework to protect the confidentiality, integrity and availability of information Council collects and/or holds.

SCOPE

This policy applies to anyone who uses or accesses Council's Corporate Information Systems, including but not limited to Alderman, employees, sub-contractors, volunteers, visitors, vendors, suppliers and business partners.

STRATEGIC PLAN ALIGNMENT

Leading Our Community

Objective 4.1	Govern in the best interests of our community
Strategy 4.1.1	Manage Council for maximum efficiency, accountability and transparency
Strategy 4.1.3	Maximise regulatory compliance in Council and the community through our systems and processes

RELATED DOCUMENTS

Aldermanic Code of Conduct

Counselling and Discipline Directive

Employee Code of Conduct

ICT Security and Usage Directives

ICT Security Standard Operating Procedures

ICT Acceptable Use Guidelines

Open Data Policy

Personal Mobile Device Directive

Working from Home Directive

Privacy Policy and Directive

Records Management Policy

DEFINITIONS

Corporate Information System means the collection of data processing systems that comprise all of the Council's information Technology systems, including but limited to external cloud/email/finance system providers, internal computing networks, and the systems and devices connected to them.

ICT means Information, Communications and Technology.

Standard Operating Procedure means a documented process to achieve a repeatable outcome.

Personal Us see ICT Acceptable Use Guidelines.

Acceptable Use see ICT Acceptable Use Guidelines.

POLICY STATEMENT

Council Commitment to Security and Appropriate Use of Information

1. Glenorchy City Council is committed to protecting the information it collects and/or holds and will maintain appropriate measures to prevent any unauthorised loss, modification or misuse of its data, whether deliberate or inadvertent.

2. Information security is the responsibility of all users of Council’s corporate information systems. All users must comply with this policy, applicable directives and any relevant legislation.

General Approach

3. All ICT equipment, systems and the information held within remain the property of the Council; access is restricted to authorised users for legitimate purposes only.

4. No external equipment is to be connected to Council's ICT systems or devices without authorisation from the General Manager after consultation with the ICT team, except where this is permitted by an ICT Security Directive.

5. All users are responsible for reporting any actual, attempted or suspected security violations including malicious emails to the ICT Service Desk.

6. The General Manager may authorise monitoring of any electronic information including email, internet usage and history, and the use of ICT equipment or information for the purpose of ensuring compliance with this policy or to meet Council's legal requirements.

7. Council will report any significant data breaches to the relevant authority as appropriate.

Information Security Framework

8. Council will develop and maintain an Information Security Framework comprising ICT Security Directives and ICT Security Standard Operating Procedures (SOPs). Directives and SOPs will be reviewed as and when needed to ensure they remain current and appropriate.

9. Revisions to ICT Security Directives must be approved by the General Manager. All affected users will be notified of any significant amendments to a directive and provided with support and training as needed to facilitate understanding and compliance.

10. Access to Council's ICT Security SOPs is restricted to authorised users while engaged on Council business only. Access will only be provided to external parties to the degree necessary to undertake legitimate activities for Council and on receipt of a signed confidentiality agreement.

Non-Compliance may result in disciplinary action

11. Anyone found to have breached this policy may be subject to investigation and disciplinary action in accordance with relevant Council policies and codes of conduct.

Authorised User Responsibility

12. Council’s ICT equipment and services must be used only for Council business activities. Limited personal use is permitted at the discretion of the authorised user’s Manager or Supervisor.

13. If there is any uncertainty as to what acceptable usage is, authorised users should consult their Manager or the ICT Service Desk before use.

14. Authorised users are not permitted to download or install any non-approved software or applications without prior approval from ICT in consultation with their supervisor.

15. Authorised users must follow all directives and procedures for handling all information received and sent, including emails.

16. Authorised users are responsible for reporting suspicious emails, access to inappropriate websites and incorrect handling of information including data privacy breaches.

Unacceptable Use

An authorised user of the Council's computer services must not:

17. Violate the rights of any person or information source that is protected by copyright, trade secret, patent or other intellectual property, or similar laws and regulations

18. Knowingly or deliberately introduce any malicious programs into the Council network or onto any storage device or computer.

19. Share or reveal their network or user account details to others or allow the use of their account by others. Circumventing identification or authentication on any computer services is expressly prohibited.

20. Use Council's computing services to engage in procuring or transmitting material that violates legislation, is in violation of applicable laws, or damages Council's reputation.

21. Attempt to breach security or otherwise intentionally or knowingly cause disruption to the Council's computer services or network communications.

BACKGROUND

Due to the constantly evolving data security landscape, it is essential that Council has a robust framework in place that both minimises risk to its information and allows it to act swiftly as new risks emerge.

This policy replaces the previous ICT Usage policies and establishes a framework to enable Council's systems and processes to be adapted as needed while still allowing an appropriate level of scrutiny and authorisation.

DOCUMENT CONTROL

Version:	1.0	**Commencement Date:**	26 October 2020
Minutes Reference	Council meeting, 26 October 2020, Item 14		
Previous Versions:	Not applicable		
Responsible Directorate	Corporate Services	**Controller:**	Manager ICT
ECM Document No.:			